EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 8/2015

Verbreitung und Verwendung von eingreifenden Überwachungs-technologien

EDPS

15. Dezember 2015

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiveren und proaktiveren Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag in rechenschaftspflichtiger Weise zu erfüllen gedenkt.

Diese Stellungnahme schließt sich an die vorherige Stellungnahme des EDSB zu der allgemeinen Datenschutzverordnung an, die darauf abzielte, die Hauptorgane der EU bei der Erzielung eines geeigneten Konsens über ein praktikables, zukunftsorientiertes Regelwerk, das die Rechte und Freiheiten natürlicher Personen untermauert, zu unterstützen. Wie in der Stellungnahme zu Mobile Health-Diensten im Frühjahr 2015 geht es auch in dieser Stellungnahme um die Herausforderung, den Datenschutz an die digitale Welt anzupassen, dem dritten Ziel der EDSB-Strategie, „um bestehende Datenschutzprinzipien für die globale digitale Arena anzupassen", auch im Lichte der Pläne der EU für einen digitalen Binnenmarkt. Sie stimmt mit dem Ansatz der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzaspekte der Verwendung neuer Technologien wie dem „Internet der Dinge", zu dem der EDSB als Vollmitglied der Gruppe beitrug, überein.

In dieser Stellungnahme geht es um die Fragen des Datenschutzes und des Schutzes der Privatsphäre, die durch die Verbreitung und Verwendung von eingreifenden Überwachungstechnologien aufgeworfen werden.

Zusammenfassung

In dieser Stellungnahme geht der EDSB auf die Fragen des Datenschutzes und des Schutzes der Privatsphäre ein, die durch die Verbreitung und Verwendung von eingreifenden Überwachungstechnologien aufgeworfen werden. Die Verwendung dieser Instrumente bedeutet automatisch die Verarbeitung personenbezogener Daten sowie einen möglichen Eingriff in die Privatsphäre: Das Hauptziel von eingreifenden Überwachungsinstrumenten ist die Infiltration von IT-Systemen aus der Ferne (in der Regel über das Internet) zur verdeckten Überwachung der Aktivitäten dieser IT-Systeme, so dass im Laufe der Zeit Daten zurück an den Nutzer der Überwachungsinstrumente gesendet werden können.

Obgleich solche Werkzeuge Instrumente für die rechtmäßige (und geregelte) Verwendung durch Strafverfolgungsbehörden und Nachrichtendienste sein können, können sie auch als „Trojanische Pferde“ zur Umgehung der Sicherheitsmaßnahmen bei der elektronischen Kommunikation und Datenverarbeitung verwendet werden.

Das Spannungsfeld zwischen dem positiven Nutzen von IKT-Werkzeugen und den negativen Auswirkungen, die ein Missbrauch der Technologie auf die Menschenrechte, und insbesondere auf den Schutz personenbezogener Daten und die Privatsphäre haben kann, muss durch einzelstaatliche und EU-Maßnahmen sowie durch alle am IKT-Sektor Beteiligten (Entwickler, Dienstleister, Verkäufer, Makler, Vertreiber und Nutzer) angegangen werden.

In dieser Stellungnahme schlägt der EDSB vor, die Bedrohung durch die Verwendung eingreifender Überwachungstechnologien mit den folgenden Maßnahmen auszuräumen:

- Es sollte eine Bewertung der bestehenden EU-Standards für IKT durchgeführt werden, mit dem Ziel, den Schutz der Menschenrechte zu stärken, insbesondere bei der Ausfuhr von Überwachungs- oder Abhörtechnologie und damit verbundenen Dienstleistungen;
- Die Verwendung und Verbreitung (einschließlich innerhalb der EU) von Überwachungs- und Abhörinstrumenten sowie verbundenen Dienstleistungen sollten einer angemessenen Regulierung unterliegen, in der das mögliche Risiko einer Verletzung der Grundrechte, insbesondere der Rechte auf Privatsphäre und Datenschutz, berücksichtigt wird;
- In Bezug auf die Ausfuhr von eingreifenden Überwachungsinstrumenten im Zusammenhang mit Technologien mit doppeltem Verwendungszweck sollten der Rat der EU, das Europäische Parlament, die Europäische Kommission und der Europäische Auswärtige Dienst (EAD) auf EU- und internationaler Ebene einheitliche und wirksamere Maßnahmen entwickeln;
- Aktuelle Maßnahmen sollten „Zero-Day-Exploits“ und Schwachstellen regulieren, um zu verhindern, dass diese für Grundrechtsverletzungen verwendet werden;
- EU-Maßnahmen zur Cybersicherheit sollten die Verbreitung von Abhör- und Überwachungstechnologien berücksichtigen und insbesondere dieses Problem im Rahmen der entsprechenden Gesetzgebung regeln;
- Investitionen in die Sicherheit im Internet und Initiativen zum „eingebauten Datenschutz“ bei neuen technologischen Lösungen sollten gefördert werden;
- Um Hinweisgebern, die zur Aufdeckung von Menschenrechtsverletzungen durch die Nutzung von Abhör- und Überwachungstechnologien beitragen, internationalen Schutz zu gewähren, sollte ein einheitlicher Ansatz erarbeitet werden.

INHALTSVERZEICHNIS

1 Der Kontext

Anfang Juli 2015[1] wurde eine italienische Firma Opfer einer groß angelegten Datenschutzverletzung. Die Angreifer stahlen eine große Menge an Daten (Berichten zufolge mehr als 400 Gigabyte) und veröffentlichten diese im Internet. Die veröffentlichten Daten umfassten interne Dokumente, Tonaufnahmen, E-Mail-Korrespondenz, Mitarbeiterpasswörter, Kundenlisten, und, was für den Zweck dieser Stellungnahme noch wichtiger ist, technische Informationen und den Quellcode einer modernen Software, die für die eingreifende Überwachung entwickelt wurde.

Den Medien zufolge[2] würde es diese eingreifende Überwachungssoftware ihrem Benutzer ermöglichen, Verschlüsselungen zu umgehen, Daten aus jeder Vorrichtung zu erheben und ein Ziel verdeckt und aus der Ferne zu überwachen[3]. Außerdem wären Strafverfolgungsbehörden und Nachrichtendienste die möglichen Kunden. Gleichzeitig wurde das Angebot auf Regierungen und Länder begrenzt, die von den Vereinigten Staaten, der EU, UN, NATO oder ASEAN nicht auf die schwarze Liste gesetzt wurden[4]. Allerdings berichten die Medien[5], dass die Software möglicherweise an „Regierungen und Nachrichtendienste von Aserbaidschan, Kasachstan, Usbekistan, Russland, Bahrain, Saudi-Arabien und den VAE, von denen viele von internationalen Menschenrechtsorganisationen für ihre aggressive Überwachung der Bürger, Aktivisten und Journalisten sowohl im Inland als auch im Ausland kritisiert wurden“ verkauft wurde.

In diesem Bereich der Cybersicherheit sind mehrere Firmen tätig und bieten entsprechende Dienstleistungen an[6]. Andere Firmen[7], die im selben Tätigkeitsbereich auftauchen, sind auf dem Markt für Cybersicherheit tätig, indem sie mit sogenannten „Exploits“ handeln (Kapitel 2.2). Diese ermöglichen die volle Ausschöpfung des Potenzials eingreifender Überwachungsinstrumente. Das Geschäftsmodell dieser Firmen sieht vor, Kunden die technischen Möglichkeiten zur Verfügung zu stellen, die für Angriffe auf IT-Systeme erforderlich sind.

Der Schwerpunkt dieser Stellungnahme liegt auf dem speziellen Fall der eingreifenden Überwachungsinstrumente, die für die [Massen-]Überwachung, die Infiltration und die Extraktion entwickelt, vermarktet und verkauft werden. Diese Instrumente werden zum Angriff auf Systeme festgelegter Ziele verwendet. Sie befasst sich nicht mit der breiteren politischen Debatte hinsichtlich einer möglichen Regulierung von Netzwerk- und Informationssicherheitstechnologien, wie der Einschränkung von Verschlüsselungen[8] und der obligatorischen Schwächung von Sicherheitssystemen durch die Verwendung von Backdoors[9].

2 Konzepte und technische Auswirkungen

Das Hauptziel von eingreifenden Überwachungsinstrumenten ist die Infiltration von IT-Systemen aus der Ferne (d. h. über das Internet) zur verdeckten Überwachung der Aktivitäten dieser IT-Systeme, so dass im Laufe der Zeit Daten zurück an den Nutzer der Überwachungsinstrumente gesendet werden können. Um zu verstehen, wie dieses Ziel erreicht wird, kann die Erklärung von eingreifenden Überwachungsinstrumenten in zwei Teile unterteilt werden: den Verwaltungsteil (Kapitel 2.1**Error! Reference source not found.**) und die Exploits (Kapitel 2.2). Anschließend werden wir einige der wichtigsten technischen Auswirkungen im Zusammenhang mit der Verwendung dieser Art von Software beleuchten (Kapitel 2.3).

2.1 Verwaltungsteil von Infiltrations- und Überwachungsinstrumenten

Im Wesentlichen kann der Verwaltungsteil von eingreifenden Überwachungsinstrumenten als moderne Software zur Steuerung der Infiltration von Zielen definiert werden und als Mittel, um den Nutzern auf benutzerfreundliche Art und Weise Exploits (siehe auch Kapitel 2.2) über Ziele zukommen zu lassen, die für sie von Interesse sind.

Zumeist verfügt der Nutzer über eine grafische Benutzeroberfläche, die ihm Folgendes ermöglicht:

- Die Eingabe der IP-Adresse (Internetprotokoll) eines mit dem Internet (Ziel) verbundenen IT-Systems zur Erhebung von Basisdaten über dieses Ziel, wie beispielsweise die Art des verwendeten Betriebssystems (BS), die verwendeten Dienste (z. B. Webserver, E-Mail-Server usw.), Ortungsdienst-Informationen usw. Dieser erste Schritt ist hilfreich, um zu ermitteln, wie dieses Ziel am besten angegriffen werden kann.

- Die Koordination und Durchführung von Angriffen auf Ziele, um diese zu infiltrieren und Daten von diesen Zielen zu erheben. Die Angriffe können in vielfältiger Form stattfinden, allerdings werden sie normalerweise unter Verwendung von Exploits durchgeführt (erörtert in Kapitel 2.2).

- Sobald das Ziel infiltriert ist, die weitere Kompromittierung des Ziels (d. h. der Versuch, lokale Sicherheitsmaßnahmen, die auf dem Ziel aktiv sind, durch die Verwendung anderer Exploits zu umgehen, um weitere Vorgänge durchführen zu können, Privilegien zu erhalten oder auf weitere von dem Ziel verarbeitete Daten zugreifen zu können) und die Installation einer kleinen Software, mit der Daten erhoben und an den Nutzer des Überwachungsinstruments geschickt werden (ähnlich einem Trojanischen Pferd[10]).

- Die Verwendung eines kompromittierten Ziels, um einen Angriff auf ein anderes verbundenes Ziel zu starten.

- Die Nachverfolgung der bereits infiltrierten Ziele und der von diesen Zielen erhaltenen/extrahierten Daten. Diese Daten sind der wichtigste Grund für die Verwendung eingreifender Überwachungsinstrumente und können alle Daten enthalten, die von dem Ziel verarbeitet werden. Hierzu zählen Browserdaten von allen Browsern, die das Ziel verwendet, gesendete und empfangene E-Mails, auf den Festplatten gespeicherte Dateien, auf die das Ziel zugreifen kann (Dateien, die sich entweder auf dem Ziel an sich oder auf anderen IT-Systemen befinden, auf die das Ziel Zugriff hat), alle aufgezeichneten Protokolle, alle auf der Tastatur verwendete Tasten (dies würde das Sammeln von Passwörtern ermöglichen), Screenshots von den Dingen, die der Nutzer des Ziels sieht, die Aufnahme von Video- und Audio-Feeds von Webcams und Mikrofonen, die mit dem Ziel verbunden sind usw.

Selbstverständlich ist diese Liste der Funktionalitäten nicht erschöpfend. Dennoch sollte sie zur Analyse der Folgen der Verwendung solcher Instrumente im Rahmen dieser Stellungnahme ausreichen.

2.2 Exploits

Bei Exploits handelt es sich um eine kleine Software, Befehlssequenzen oder Daten, die entwickelt werden, um aus einer Fehlfunktion/Schwachstelle in der Software des Ziel-IT-Systems Nutzen zu ziehen und somit eine unbeabsichtigte und unvorhergesehene Reaktion dieser Software auszulösen. Oftmals ist das Ziel, das Exploit auf eine Weise zu entwickeln, dass die automatische Reaktion der angegriffenen Software dazu führt, dem Angreifer eine gewisse Kontrolle über oder Zugriff auf das Ziel zu ermöglichen.

Ein Exploit kann nur dann existieren, wenn in einer Software eine Fehlfunktion/Schwachstelle vorhanden ist. Fehlfunktionen/Schwachstellen werden im Laufe der Zeit von Wissenschaftlern, Softwareherstellern und der Öffentlichkeit festgestellt und können in jeder Software auftreten, wie beispielsweise MS Windows, Linux, MAC OS X, Android, Apple iOS, Blackberry OS oder jedem anderen Betriebssystem, und in Software, die mit dem und über das Internet verwendet wird, wie Adobe Flash (wird auf einer Vielzahl von Websites, einschließlich Youtube, Google usw. verwendet), Firefox, Safari, Internet Explorer usw.

Sobald ein Softwarehersteller über eine Fehlfunktion/Schwachstelle bei seinem Produkt informiert wird, kann dieser normalerweise das Problem beheben und der Öffentlichkeit eine neue Version der Software zur Verfügung stellen. Sobald die aktualisierte Software auf einem IT-System installiert ist, kann dieses IT-System nicht mehr durch das entsprechende Exploit beeinträchtigt werden.

Bei „Zero-Day-Exploits“ handelt es sich um einen Begriff, mit dem Exploits beschrieben werden, die eine Fehlfunktion/Schwachstelle verwenden, die dem Softwarehersteller unbekannt ist und für die es keine bestehende Korrekturmaßnahme gibt. Diese Arten von Exploits sind nützlich, da sie sehr wahrscheinlich für einen erfolgreichen Angriff auf ein System verwendet werden können, das die entsprechende fehlerhafte Software verwendet. Die Kosten für Exploits können 100 000 Euro übersteigen. Dies hängt von zahlreichen technischen Faktoren ab[11].

Im Fall von HT handelte es sich um ein Exploit im Zusammenhang mit der Adobe Flash-Software, über das in den Medien ausführlich berichtet wurde[12]. Dieses Exploit betraf die neueste Version der Adobe Flash-Software, die zu diesem Zeitpunkt auf einer Vielzahl von Plattformen und Browsern installiert war. Es ermöglichte dem Angreifer, jedes gewünschte Programm auf dem Ziel auszuführen. Ein glaubwürdiges Szenario für einen Angriff hätte wie folgt ausgesehen:

- Ein Nutzer surft im Internet und verwendet auf seinem Computer eine gefährdete Version von Adobe Flash. Der Nutzer greift auf eine Website mit Adobe Flash-Inhalt (beispielsweise ein Video) zu, der das Exploit enthält;

- der Computer des Nutzers spielt den Adobe Flash-Inhalt ab und führt zur gleichen Zeit das Exploit aus, ohne sichtbares Anzeichen für den Nutzer;

- der Angreifer (derjenige, der den Adobe Flash-Inhalt mit dem Exploit präpariert hat) hat nun Zugriff auf den Computer des Nutzers und verfügt über dieselben Rechte wie der Nutzer;

- der Angreifer kann nun zusätzliche Exploits ausführen, um weiteren Zugriff auf den Computer des Nutzers zu erhalten und/oder kann Software installieren, die ihm Daten zurückübermittelt.

Für Exploits wie für das eben genannte existiert ein großer Markt[13], da sie im Zusammenhang mit Überwachungsinstrumenten äußerst hilfreich sind. Ohne diese Exploits wäre die Infiltration eines IT-Systems zudem weitaus schwieriger und würde eine aktivere Teilnahme eines Benutzers erfordern, der bereits Zugriff auf das Ziel hat. Die betroffenen Firmen haben großes Interesse daran, dass die Kenntnis solcher Fehlfunktionen/Schwachstellen sorgfältig unter Verschluss gehalten wird.

2.3 Technische Auswirkungen

Angesichts der Datenverletzungen, die im Internet umfassend bekannt gemacht wurden[14], ist eingreifende Überwachungssoftware nun für die breite Öffentlichkeit zugänglich. Laut Presse *„wurde ausreichend Code veröffentlicht, damit die Software von jedermann gegen ein gewünschtes Ziel eingesetzt werden kann"; „… ist es nicht mehr möglich, zu kontrollieren, wer die Technologie verwendet", „Wir sind der Meinung, dass diese Situation extrem gefährlich ist"*[15].

Es sei darauf hingewiesen, dass Softwarehersteller, sobald ein Exploit (und damit verbundene Fehlfunktionen/Schwachstellen) publik wird, Patches oder neue Versionen ihrer Software veröffentlichen, die nicht für dieselben Angriffe anfällig sind. Vorausgesetzt, die Nutzerbasis installiert diese neuen Versionen oder Patches, sind die Nutzer vor diesen konkreten Problemen sicher. Dies zeigt, wie wichtig es für alle (Privatunternehmen, öffentliche Einrichtungen oder Einzelpersonen) ist, den Überblick über die verwendete Software zu behalten und ihre IT-Systeme schnell zu aktualisieren.

Nichtsdestotrotz würden Anbieter und Nutzer dieser Überwachungsinstrumente im eigenen Interesse normalerweise keine Informationen über bestehende Fehlfunktionen/Schwachstellen offenlegen: Anbieter werden auf diese Weise verfahren, um sicherzustellen, dass ihre Infiltrationssoftware so lange wie möglich effektiv bleibt (und sie somit ihren Geschäftserfolg sichern). Nutzer dieser Überwachungsinstrumente möchten ihre Cyberfähigkeiten wahren, wobei dies auf Kosten der Sicherheit und Privatsphäre von Hunderttausenden, wenn nicht gar Millionen von Internetnutzern geht. Weniger seriösen Gruppen (Gruppen des organisierten Verbrechens, böswilligen Hackern usw.) dürften die gleichen Fehlfunktionen/Schwachstellen nur allzu gut bekannt sein, so dass sie diese zu ihrem eigenen Vorteil nutzen können.

Außerdem unterscheiden eingreifende Überwachungsinstrumente nicht zwischen den verschiedenen Nutzern eines bestimmten Ziels: Sobald ein Ziel kompromittiert ist, werden alle Daten, die das Überwachungsinstrument anfordert, erhoben, unabhängig von der Person, die das Ziel verwendet.

Abhängig davon, auf welche Art und Weise die Angriffe auf Ziele durchgeführt werden, gibt es zudem möglicherweise unbeabsichtigte Opfer, die dabei gänzlich andere IT-Systeme verwenden.

- Um noch einmal das Beispiel aus Abschnitt 2.2 aufzugreifen: Ein Nutzer, der im Internet surft, könnte unbewusst über einen Adobe Flash-Inhalt stolpern, der Exploits

enthält, und zu einem Opfer eines unrechtmäßigen Angriffs werden, der seine Sicherheit und Privatsphäre gefährdet.

- Um ein bestimmtes Ziel erfolgreich zu kompromittieren, könnte es für den Nutzer des eingreifenden Überwachungsinstruments erforderlich sein, ein anderes IT-System zu kompromittieren, von dem bekannt ist, dass das Ziel darauf zugreift (um Zugriff auf das Online-Banking-Konto eines Nutzers zu erhalten, könnte ein Angreifer beispielsweise zunächst die Video-on-Demand-Website desselben Nutzers oder den Facebook-Account eines seiner Freunde anvisieren). Dies würde wiederum die Kompromittierung der Sicherheit und Privatsphäre von Personen bedeuten, die in keinem Zusammenhang mit der Untersuchung stehen, abgesehen davon, dass sie das Pech haben, die Nutzer eines mit dem Ziel verbundenen IT-Systems zu sein.

Abhängig von technischen Spezifikationen und dem spezifischen Kontext können eingreifende Überwachungsinstrumente unter gewissen Umständen Instrumente für die rechtmäßige (und geregelte) Verwendung durch Strafverfolgungsbehörden oder Nachrichtendienste sein. Zur Umgehung von Sicherheitsmaßnahmen bei der elektronischen Kommunikation können sie auch als „Trojanische Pferde“ verwendet werden (z. B. Netzwerkverschlüsselung): Sobald der Angriff auf ein Ziel erfolgreich ist, werden die Überwachungsinstrumente auf die Daten des Ziels zugreifen. Dies geschieht noch vor der Übermittlung dieser Daten ins Internet, also bevor die Daten mit einer Netzwerkverschlüsselung versehen werden würden. Dies hätte natürlich zur Folge, dass jegliche Verschlüsselung, die von dem Ziel verwendet wird, nutzlos wäre.

3 Die Rolle des EDSB und anderer Datenschutzbehörden

Die Verordnung (EG) Nr. 45/2001 überträgt dem EDSB die Pflicht zur Beratung der Organe und Einrichtungen der EU in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten[16]. Gemäß derselben Verordnung ist es dem EDSB auch gestattet, aus eigener Initiative Stellungnahmen anzunehmen, um auf Risiken hinzudeuten, die sich auf die Rechte auf Privatsphäre und Datenschutz der Bürger auswirken. In dieser Stellungnahme geht der EDSB auf die Fragen des Datenschutzes und des Schutzes der Privatsphäre ein, die durch die Verbreitung von Überwachungsinstrumenten und -software aufgeworfen werden, da die Verwendung dieser Instrumente automatisch die Verarbeitung personenbezogener Daten sowie einen möglichen Eingriff in das Recht auf Privatsphäre bedeutet.

Parallel hierzu gilt die Richtlinie 95/46/EG auch „*für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen*“[17].

Die Verwendung eingreifender Überwachungsinstrumente umfasst sicherlich die Verarbeitung personenbezogener Daten. Tatsächlich umfasst der Begriff „personenbezogene Daten“ unter anderem jegliche Informationen, Kommunikation, Metadaten, Aktivitäten und Bewegungen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Es handelt sich um Informationen, wie sie offensichtlich von Überwachungssystemen verarbeitet werden. Außerdem wird das Erheben, Speichern oder Abfangen von Daten als Verarbeitung dieser Daten erachtet. Sobald die Verarbeitung dieser Daten automatisch von Überwachungsinstrumenten durchgeführt wird und weiterhin in den Anwendungsbereich der

Richtlinie 95/46/EG fällt, gelten daher deren Vorschriften und Grundsätze (wie durch nationale Rechtsvorschriften und die Verordnung (EG) Nr. 45/2001 eingeführt).

Daraus ergibt sich insbesondere, dass selbst wenn andere Rechts- oder Verwaltungsvorschriften (zum Beispiel hinsichtlich der Verbreitung, der Ausfuhr und der Verwendung der Technologie) eingehalten werden, die Grundsätze des Datenschutzrechts dennoch gewahrt werden müssen. Mit anderen Worten: Wird eine Technologie oder eine Vorrichtung zum Verkauf an die Öffentlichkeit und zur Verwendung zugelassen, beeinflusst diese Zulassung keineswegs die Auswirkungen, die eine solche Technologie auf die Privatsphäre natürlicher Personen haben könnte, und auch nicht die Tatsache, dass jegliche Verwendung im Einklang mit den Bestimmungen zum Schutz der Privatsphäre und zum Datenschutz stehen muss.

Neben ihrer beratenden Funktion in Bezug auf administrative oder regulatorische Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten können der EDSB sowie andere Datenschutzbehörden auf EU-Ebene daher eingreifen, um auf spezielle Risiken hinzuweisen, die sich im Zusammenhang mit der Verwendung von eingreifender Überwachungstechnologie für die Rechte der Bürger ergeben können.

In diesem Zusammenhang sei darauf hingewiesen, dass das Abhören von Kommunikation, die Speicherung personenbezogener Informationen und die Analyse von Datensätzen natürlich schwerwiegende Auswirkungen auf die Privatsphäre eines Jeden und auf den Schutz personenbezogener Daten haben.

4 Bewertung der betroffenen Maßnahmen

Im nächsten Kapitel wird kurz Folgendes dargelegt:

1. *Die Herausforderungen, die sich im Zusammenhang mit der Verwendung von Überwachungs- und Abhörtechnologien ergeben, die angegangen werden sollten;*
2. *Die bestehenden Richtlinien in Bezug auf eingreifende Überwachungstechnologien;*
3. *Mögliche Ergebnisse sowie ein zukunftsorientierter Ansatz für weitere Regelungen.*

4.1 Herausforderungen

Einige technologische Systeme können zur Verletzung von Menschenrechten verwendet werden. Hierzu zählen Zensur, Überwachung, unbefugter Zugriff auf Vorrichtungen, Störungen, Abhörmaßnahmen oder Verfolgung natürlicher Personen. Diese Verletzungen können von privaten oder öffentlichen Einrichtungen (einschließlich Strafverfolgungsbehörden und Regierungen) vorgenommen werden. Cyberangriffe, illegale Abhörmaßnahmen, Massenüberwachung durch staatliche Stellen sowie Angriffe auf Computersysteme sind alle Beispiele für Tätigkeiten, die durch die Verwendung spezieller IKT-Geräte, -Instrumente oder sogar -Informationen durchgeführt werden können (z. B. Wissen über Software-Schwachstellen).

Auf der anderen Seite können IKT-Instrumente auch Werkzeuge sein, die zur Verbreitung von Ideen und Informationen sowie zur Organisation gesellschaftlicher Bewegungen beitragen können, insbesondere in Regionen mit autoritären Regimen. Das Internet ist zudem ein Forum, das den Menschen zahlreiche Möglichkeiten zum Daten-, Informations- und Wissensaustausch bietet. Daher können sich IKT äußerst positiv auf die Verbesserung der Menschenrechte auswirken. So können beispielsweise Menschenrechtsaktivisten die Verschlüsselung verwenden, um jegliche Infiltration, Abhörmaßnahme oder Überwachung durch staatliche Stellen zu vermeiden. In diktatorischen Regimen können einige Technologien außerdem von Journalisten zur Umgehung der Zensur verwendet werden. Daher ist der Tatsache Rechnung zu tragen, dass die Verwendung von IKT dem Schutz der Menschenrechte dienen und digitale Rechte und Freiheiten erleichtern kann, einschließlich den Schutz der Vertraulichkeit, Privatsphäre und personenbezogener Daten.

Das Spannungsfeld zwischen dem positiven Nutzen von IKT-Werkzeugen und den negativen Auswirkungen, die ein Missbrauch der Technologie auf die Grundrechte haben kann, und insbesondere auf den Schutz personenbezogener Daten und die Privatsphäre, muss durch einzelstaatliche und EU-Maßnahmen und durch alle am IKT-Sektor Beteiligten angegangen werden (Entwickler, Dienstleister, Verkäufer, Makler, Vertreiber und Nutzer).

In einer Situation verstärkter Sicherheitsbedenken können sich Nachrichtendienste und Polizei für die Verwendung von Technologie entscheiden (einschließlich eingreifender Überwachungstechnologie), um ihre Ermittlungen zielgerichteter und effektiver durchführen zu können. In diesem Zusammenhang ist es uns nicht möglich, die Verwendung von „Big Data“ als ein Ermittlungsinstrument auszuschließen, da dieses bei der Verknüpfung von Informationen und Beweisen aus verschiedenen Quellen effektiv ist. In diesem Zusammenhang ist darauf hinzuweisen, dass die derzeitigen Rechtsvorschriften zum Datenschutz, selbst in einer neu überarbeiteten Fassung, nicht ausreichend spezifiziert sind, um alle Probleme anzugehen, die im Rahmen von Ermittlungen und Strafverfolgung durch die Verwendung von Technologien, die sich auf die Privatsphäre auswirken, aufgeworfen werden.

Mit der heutigen weltweiten Vernetzung hat die Cybersicherheit eine globale Dimension, die über die Grenzen der EU hinausgeht. Diese globale Dimension macht eine wirksame Cybersicherheit zu einer erheblichen Herausforderung, einer Herausforderung, die jedoch angenommen werden muss, da Cybersicherheit ein wesentliches Element des Datenschutzes ist. Die Rechte auf Privatsphäre und Datenschutz sowie Cybersicherheit verfolgen dasselbe Ziel: Die Gewährleistung eines hohen Maßes an Cybersicherheit wird tatsächlich zur Verbesserung der Sicherheit aller verarbeiteten Daten beitragen, einschließlich personenbezogener Daten.

Allerdings darf Cybersicherheit nicht als Ausrede für eine unverhältnismäßige Verarbeitung personenbezogener Daten herangezogen werden, wie im Fall eingreifender Überwachungsinstrumente. Datenschutzprinzipien wie Notwendigkeit und Verhältnismäßigkeit tragen dazu bei, die rechtmäßige Verwendung von Infiltrations- und Überwachungstechnologien zu regeln. Zudem wird durch den „eingebauten Datenschutz“ die Einbeziehung der Datenschutzvorkehrungen in die Technologie in der Entwicklungsphase gefördert. Ebenso stellen die „datenschutzfreundlichen Voreinstellungen“ sicher, dass die Voreinstellungen der Technologie dem Datenschutz entsprechen, ohne konkrete Auswahlmöglichkeiten durch den Nutzer.

Auch in Bezug auf das Vertrauen, die Integrität von Transaktionen und die Entwicklung des digitalen Binnenmarktes, der intelligenten Netze und des „Internets der Dinge“ ist die Sicherheit der Daten, Systeme und Netzwerke von erheblicher Bedeutung. Ein abgeschwächter Datenschutz, um eine allgegenwärtigere Überwachung zu erlauben, würde das Vertrauen zerstören und den EU-Binnenmarkt und die Digitale Agenda der EU untergraben. Es ist verständlich, dass Überwachungs- und Strafverfolgungsbehörden die zur Kriminalitätsbekämpfung erforderlichen Mittel benötigen, auch im Internet. Allerdings ist für jede neue Maßnahme die Notwendigkeit und Verhältnismäßigkeit der geplanten Maßnahme im Voraus zu bewerten. Außerdem müssen im Vorhinein fundierte Belege hinsichtlich der Notwendigkeit dieser Maßnahmen erbracht werden.

Privatsphäre und Datenschutz stehen weder im Widerspruch zu Wirtschaftswachstum und internationalem Handel noch zu Cybersicherheit oder verbesserten Leistungen und Produkten. Sie sind vielmehr Teil einer qualitativ hochwertigen Lösung.

4.2 Bewertung von Maßnahmen im Zusammenhang mit Überwachungs- und Abhörtechnologien

Die Verarbeitung personenbezogener Daten für Strafverfolgungszwecke im Rahmen des EU-Rechts durch die zuständigen Behörden sollte auch die in der Charta der Grundrechte der EU verankerten Standards und Schutzmechanismen berücksichtigen. In Artikel 7 der Charta ist das **Recht auf Privatsphäre** verankert, ein Recht, für das der Schutz personenbezogener Daten von grundsätzlicher Bedeutung sein kann. Daher sollte der Eingriff in das virtuelle Domizil über Spyware, Exploits oder ähnliche Vorrichtungen als Verletzung der Privatsphäre erachtet werden. In diesem Zusammenhang sollte das „virtuelle Domizil“ mit demselben Respekt geschützt werden wie das physische Domizil[18]. Das **Recht auf den Schutz personenbezogener Daten** ist in Artikel 8 der Charta verankert. Demnach haben natürliche Personen ein Recht auf Einhaltung bestimmter Garantien, sobald ihre personenbezogenen Daten verarbeitet werden. Daher sollte für die Verwendung von Überwachungsinstrumenten eine spezielle Gesetzgebung gelten, in der die vertretbaren Grenzen der Verbreitung und Verwendung solcher Technologien bestimmt und die erforderlichen Schutzmechanismen für eine solche Verwendung festgelegt werden.

Daher werden sich die in der EU verwendeten Überwachungsinstrumente und -software auf diese zwei Grundrechte natürlicher Personen auswirken. Auf der anderen Seite sollte die EU die Auswirkungen ihrer Maßnahmen auf die Grundrechte natürlicher Personen in Drittländern messen. Um zu verhindern, dass mit zweierlei Maß gemessen wird, wenn es darum geht, die Folgen der EU-Maßnahmen innerhalb und außerhalb der EU zu bewerten, sollte ohne Frage ein einheitlicher Ansatz angeregt werden.

Die Gesetzgebung der Mitgliedstaaten sieht die Rechtswidrigkeit der Verwendung von IKT-Werkzeugen unter bestimmten Umständen vor. Bereits in Artikel 6 des **Budapester Übereinkommens über Cyberkriminalität** wird das Problem des Herstellens, Verkaufens, Beschaffens zwecks Gebrauchs, Einführens, Verbreitens oder anderweitigen Verfügbarmachens einer Vorrichtung, einer Software oder eines Computerpassworts oder eines Zugangscodes oder ähnlicher Daten mit dem Vorsatz, sie zur Begehung einer Straftat zu verwenden, thematisiert. Allerdings kann der Anwendungsbereich dieser Bestimmung möglicherweise nicht so angepasst werden, dass er für alle Überwachungs- und Abhörtechnologien gilt. Außerdem werden in dieser Bestimmung rechtmäßige Überwachungs- oder Abhörhandlungen nicht untersagt (z. B. durch gesetzlich befugte

Strafverfolgungsbehörden). Somit bleibt teilweise unklar, ob die wirksame Anwendung dieser Bestimmung das Problem von Überwachungs- oder Abhörinstrumenten, die Menschenrechtsverletzungen auf eine Weise ermöglichen, die auch natürliche Personen der EU betreffen können, in vollem Umfang und ordnungsgemäß ausräumen kann.

Die **Ausfuhr von Überwachungs- und Abhörtechnologien** kann auch der sogenannten „Dual-Use"-Verordnung (EG) Nr. 428/2009[19] unterliegen. Gemäß dieser Verordnung kann die Ausfuhr schädlicher Technologien an Drittländer kontrolliert werden. Der EDSB begrüßt die Tatsache, dass sich die Vertragsstaaten des Wassenaar-Arrangements im Dezember 2013 auf die Einführung von Ausfuhrkontrollen in Bezug auf „Infiltrationssoftware" und „IP-Netzwerk Überwachungssysteme" einigten.

Allerdings konnte mit der EU-Regelung zum doppelten Verwendungszweck das Problem der Ausfuhr aller IKT-Technologien[20] in ein Land, in dem nicht alle angemessenen Garantien hinsichtlich der Verwendung dieser Technologie gegeben sind, nicht vollständig ausgeräumt werden. Somit sollte die derzeitige Überarbeitung der „Dual-Use"-Verordnung als Chance gesehen werden, die Ausfuhr von potenziell schädlichen Vorrichtungen, Diensten und Informationen in Drittländer, die ein Risiko für die Menschenrechte darstellen, einzuschränken.

Im Zusammenhang mit dem doppelten Verwendungszweck sollten Standards entwickelt werden, um zu bewerten, wie die IKT oder die betreffenden Informationen verwendet werden könnten und welche möglichen Auswirkungen sie auf die Grundrechte in der EU hätten[21]. Es sollte eine Analyse der Situation in dem Drittland hinsichtlich des tatsächlichen Schutzes der Menschenrechte oder der Wahrung der Freiheiten der Menschen durchgeführt werden, um beurteilen zu können, ob und unter welchen Umständen eine Ausfuhrgenehmigung erteilt werden sollte. Zudem ist eine Bewertung des Zusammenhangs, in dem die Technologien verwendet werden, unbedingt erforderlich, um deren Auswirkungen auf die Menschenrechte zu beurteilen.

Dennoch kann sich die EU-Verordnung zum doppelten Verwendungszweck nicht mit allen Fragen hinsichtlich der Verbreitung und Verwendung von Überwachungstechnologien befassen. Ein weiteres Instrument, das einen Rahmen für die Tätigkeiten des Strafverfolgungsektors bilden sollte, ist die **zukünftige Datenschutzrichtlinie**, die für den Strafverfolgungsektor gilt[22]. Bei der Verwendung von IKT-Technologien durch Strafverfolgungsbehörden müssen die Grenzen der Bestimmungen dieser Richtlinie und deren nationale Umsetzung eingehalten werden.

Folglich ist der effektive Schutz der IKT-Systeme vor jeglichen Angriffen oder illegalen Abhörmaßnahmen für den Schutz der Grundrechte auf Privatsphäre und Datenschutz natürlicher Personen in der EU unbedingt erforderlich. Die **Digitale Agenda der EU** enthält bereits eine Reihe von Maßnahmen, die auf die Verbesserung der Cybersicherheit abzielen und eine bessere Widerstandsfähigkeit der IKT-Systeme gegenüber Vorfällen, die ihre Sicherheit verletzen könnten, vorsehen.

In diesem Zusammenhang schlug die EU eine **Cybersicherheitsstrategie** vor[23], bei der die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) besser involviert sein soll und in deren Rahmen IT-Notfallteams (Computer Emergency Response Teams, CERTs) eingerichtet und neue Rechtsvorschriften[24] und Maßnahmen[25] vorgeschlagen werden, um Sicherheitsbedrohungen und -vorfällen entgegenzuwirken. Bei der

Cybersicherheitsstrategie der EU sollte die Möglichkeit berücksichtigt werden, dass die Verwendung von IKT-Technologien sowohl die Grundrechte in der EU als auch in Drittländern verletzen könnte. Daher sollte ein einheitlicher Ansatz hinsichtlich der Verbreitung von IKT-Überwachungs- und Abhörtechnologien im Rahmen der Cybersicherheitsstrategie verabschiedet werden.

Schließlich ist auch der **Rahmen für den Datenschutz** ein hilfreiches Instrument, das verwendet werden könnte, um die Sicherheit und Verletzung von Grundrechten anzusprechen. Da das Abhören und die Überwachung personenbezogener Daten als Reaktion die Anwendung des Rechtsrahmens für den Datenschutz bewirken wird, kann die bloße Einhaltung von Ausfuhr-, Sicherheits-, Handels- oder Schutzgesetzen durch eine IKT-Technologie den Nutzer nicht davon entbinden, den in den nationalen Datenschutzvorschriften oder in der Verordnung (EG) Nr. 45/2001 niedergelegten Datenschutzprinzipien nachzukommen.

Die **Verpflichtung zur sicheren Verarbeitung personenbezogener Daten** ist bereits in der Richtlinie 95/46/EG verankert[26]. Der mit der allgemeinen Datenschutzverordnung geschaffene zukünftige Rechtsrahmen sieht zudem neue Vorschriften vor, die dazu dienen können, die Sicherheit und den Schutz personenbezogener Daten anzugehen. Die Grundsätze des *„eingebauten Datenschutzes“* und der *„datenschutzfreundlichen Voreinstellungen“* sollten die Firmen dazu veranlassen, die Verwendung ihrer IKT-Technologien so zu gestalten, dass der rechtmäßige Zweck einer Organisation besser erfüllt werden kann. Dies geschieht durch eine Einschränkung der Datenerhebung auf das Notwendige oder durch ein angemessenes Abstellen auf die Personen und Kommunikation, die überwacht werden sollen. Die obligatorische Berichterstattung über Datenschutzverletzungen ist ein weiteres Instrument, das zur Identifizierung von Schwachstellen eines IKT-Systems mit mangelnder Sicherheit hinsichtlich einer bestimmten Verarbeitung personenbezogener Daten beitragen könnte.

4.3 Das weitere Vorgehen

Angesichts der oben genannten Ziele sollte gegebenenfalls eine spezielle Gesetzgebung die Anwendung von Datenschutzvorkehrungen für Ermittlungs- und Durchsetzungsmaßnahmen regeln, die auf Technologie angewiesen sind. Obgleich Gesetzgebung und Technologieentwicklung mit unterschiedlicher Geschwindigkeit voranschreiten, sollte eine solche Gesetzgebung so zukunftsorientiert wie möglich sein. Insbesondere sollte sie auf einer Bewertung der Technologien basieren und berücksichtigen, dass – wiewohl diese Technologien noch nicht für nachrichtendienstliche und polizeiliche Ermittlungen verwendet werden – sie bereits getestet werden und auf dem Markt erhältlich sind. Gleichzeitig sollte die Gesetzgebung technologisch neutral bleiben und den Schwerpunkt auf die Auswirkungen legen, die die Technologie auf den Datenschutz haben kann, um die Anwendung bestimmter Schutzmechanismen anzuordnen. Solche Maßnahmen sollen die rechtmäßige Forschung weder verhindern[27] noch den Zugriff auf und die Übermittlung von Informationen unnötig einschränken.

Der Rückgriff auf Überwachungsinstrumente wird die Interessen zahlreicher Interessengruppen beeinflussen: Softwareentwickler und -hersteller, Strafverfolgungsbehörden und die Internet-Gemeinschaft insgesamt. Daher ist es entscheidend, dass die Debatte hinsichtlich der zu ergreifenden rechtlichen Maßnahmen die umfassende Konsultation mit diesen Interessengruppen ermöglicht. Insbesondere sollten

Grundsätze wie der *„eingebaute Datenschutz“* und die *„datenschutzfreundlichen Voreinstellungen“* Teil der Diskussion sein, da Ersterer den Einbau von Datenschutzvorkehrungen in die Technologie ermöglicht (und somit seine Auswirkungen auf das Leben der Bürger abschwächt) und Letztere dafür sorgen, dass selbst Personen, die sich weniger Gedanken um ihre Privatsphäre machen, ein angemessenes Schutzniveau erhalten. Wenn wir verstehen, dass Firmen mehr Rechtssicherheit benötigen, tragen diese im Gegenzug auch eine moralische Verantwortung, wenn sie sich an derartigen Aktivitäten beteiligen.

Angesichts des oben Aufgeführten besteht eine wesentliche Herausforderung darin, auf Technologie basierende, wirksame Ermittlungsinstrumente zu gewährleisten und gleichzeitig die Rolle des Internets als ein Forum für freie Meinungsäußerung und demokratische Interaktion zwischen den Bürgern zu wahren. Bürger werden den Schutz vor äußeren Bedrohungen zunehmend fordern (z. B. Kriminalität und Terrorismus). Gleichzeitig werden sie jedoch eine berechtigte Erwartung haben, dass verstärkte Sicherheit nicht auf Kosten ihrer Grundfreiheiten erfolgt. Die Anwendung von Grundsätzen wie Notwendigkeit und Verhältnismäßigkeit stellt sicher, dass Ermittlungen und polizeiliche Tätigkeiten zielgerichtet sind und eingeschränkte Auswirkungen auf die Privatsphäre der Bürger haben.

Alle im Bereich der Cybersicherheit Beteiligten sind gefordert (Forscher, Strafverfolgungsbehörden, IT-Notfallteams (Computer Emergency Response Teams, CERTs), private und öffentliche Einrichtungen usw.), Informationen über Softwarefehler/-schwachstellen und Informationen über Sicherheitsvorfälle und -verletzungen auszutauschen, um eine möglichst effiziente, effektive und umfassende Durchsetzung von geeigneten Software- und Sicherheitsmaßnahmen sicherzustellen. In dieser vernetzten Welt hängt die Sicherheit eines jeden Einzelnen von der Sicherheit aller ab. Durch gemeinsames und koordiniertes Handeln können wir die Cybersicherheit für alle am wirksamsten gewährleisten.

Die Enthüllungen über die Massenüberwachung gaben zudem Anlass zu ernsthaften Bedenken dahingehend, ob der Schutz der betroffenen Personen in der EU gewahrt wird. Die nationale Sicherheit kann keine Rechtfertigung für eine ungezielte, willkürliche und geheime Überwachung sein. Daher sollte die EU einen einheitlichen, globalen Ansatz verabschieden: Da die von Edward Snowden aufgedeckten Überwachungspraktiken in den Vereinigten Staaten Anlass zu Bedenken hinsichtlich ihrer Vereinbarkeit mit den Grundrechten der betroffen Personen in Europa geben, sollten die Mitgliedstaaten die Möglichkeit vorsehen, Hinweisgebern internationalen Schutz zu gewähren, einschließlich das Recht auf Asyl.

5 Schlussfolgerungen

Auf der Grundlage des oben Ausgeführten ist der EDSB der Meinung, dass die Bedrohung durch die Verwendung eingreifender Überwachungstechnologien mit den folgenden Maßnahmen ausgeräumt werden könnte:

- Es sollte eine Bewertung der bestehenden EU-Standards für IKT durchgeführt werden, mit dem Ziel, den Schutz der Menschenrechte zu stärken, insbesondere bei der Ausfuhr von Überwachungs- oder Abhörtechnologie und damit verbundenen Dienstleistungen;
- Die Verwendung und Verbreitung (einschließlich innerhalb der EU) von Überwachungs- oder Abhörinstrumenten sowie verbundenen Dienstleistungen sollten einer angemessenen Regulierung unterliegen, in der das mögliche Risiko einer Verletzung der Grundrechte, insbesondere der Rechte auf Privatsphäre und Datenschutz, berücksichtigt wird;
- In Bezug auf die Ausfuhr von eingreifenden Überwachungsinstrumenten im Zusammenhang mit Technologien mit doppeltem Verwendungszweck sollten der Rat der EU, das Europäische Parlament, die Europäische Kommission und der Europäische Auswärtige Dienst (EAD) auf EU- und internationaler Ebene einheitliche und wirksamere Maßnahmen entwickeln;
- Aktuelle Maßnahmen sollten „Zero-Day-Exploits“ und Schwachstellen regulieren, um zu verhindern, dass diese für Grundrechtsverletzungen verwendet werden;
- EU-Maßnahmen zur Cybersicherheit sollten die Verbreitung von Abhör- und Überwachungstechnologien berücksichtigen und insbesondere dieses Problem im Rahmen der entsprechenden Gesetzgebung regeln;
- Investitionen in die Sicherheit im Internet und Initiativen zum „eingebauten Datenschutz“ bei neuen technologischen Lösungen sollten gefördert werden;
- Um Hinweisgebern, die zur Aufdeckung von Menschenrechtsverletzungen durch die Nutzung von Abhör- und Überwachungstechnologien beitragen, internationalen Schutz zu gewähren, sollte ein einheitlicher Ansatz erarbeitet werden.

Brüssel, den 15. Dezember 2015

(**gezeichnet)**

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

Anmerkungen

[1] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[2] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/.

[3] https://www.hackingteam.com/images/stories/galileo.pdf.

[4] https://www.hackingteam.com/index.php/customer-policy.

[5] http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

[6] https://www.finfisher.com/FinFisher/company.html.
https://www.finfisher.com/FinFisher/products_and_services.html.
http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked.

[7] https://www.zerodium.com/about.html.

[8] http://www.theverge.com/2015/11/10/9703526/tim-cook-encryption-uk-investigatory-powers-bill.

[9] https://de.wikipedia.org/wiki/Backdoor.

[10] http://malware.wikia.com/wiki/Trojan.

[11] http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/.

[12] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[13] http://arstechnica.com/security/2015/07/hacking-team-leak-releases-potent-flash-0day-into-the-wild/.

[14] http://www.engadget.com/2015/07/09/how-spyware-peddler-hacking-team-was-publicly-dismantled/,
http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked

[15] Pressemitteilungen von Hacking Team vom 08.06.2015, 14.06.2015 und 22.06.2015 (http://www.hackingteam.it/index.php/about-us).

[16] Artikel 43 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr

[17] Artikel 3 Absatz 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

[18] Siehe beispielsweise die Entscheidung des Bundesverfassungsgerichts vom 29. Februar 2009, BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html;jsessionid=EFB9C866CBD6E6D7E83473B4EC6B164B.2_cid393.

[19] Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck.

[20] Technologien, Informationen, Exploits, Software und Vorrichtungen mit möglichen Auswirkungen auf die Menschenrechte sollten alle der Regelung zum doppelten Verwendungszweck unterliegen, um Defizite und Lücken dieser Regelung zu vermeiden.

[21] Siehe beispielsweise Maßnahme 6, wie von M. SCHAAKE, Mitglied des Europäischen Parlaments, vorgeschlagen, in der die Anwendung von EU-„Know-your-Customer"-Leitlinien für Ausfuhren angeregt wird: http://www.marietjeschaake.eu/2015/10/marietje-schaake-proposes-12-actions-to-remedy-human-rights-shortcomings-in-the-eus-dual-use-regulation/.

[22] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

[23] Cybersicherheitsstrategie der Europäischen Union: Ein offener, sicherer und geschützter Cyberraum, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

[24] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union - COM(2013) 48 endgültig - 7.2.2013 - DE. Am 8. Dezember haben die Kommission, der Rat und das Parlament eine Einigung zu diesem Text erzielt: siehe http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

[25] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security%23Our%20Actions

[26] Artikel 17.

[27] Einschließlich Bug-Bounty-Programme, die als Anreiz für Personen gedacht sind, Softwareunternehmen Informationen über Schwachstellen zur Verfügung zu stellen.